Jamaica
Cyber Threat Report
2021-2025

Roadmap to Resiliency

January 2026

JAMAICA
CYBER THREAT REPORT
2021-2025

ROADMAP TO RESILIENCY

ABOUT DPO Caribbean

DPO Caribbean is dedicated to advancing digital policy solutions for the Caribbean. We support governments, institutions, and stakeholders in navigating the social, economic, privacy and security challenges of the digital age. Through evidence-based research, policy analysis, and regional collaboration, we provide advisory services in digital services, data protection, cybersecurity, and AI governance, helping to shape inclusive, resilient, and future-ready digital frameworks that protect citizens and enable sustainable digital transformation across the Caribbean.

Visit us at https://dpocaribbean.com/

AUTHOR

Corlane Barclay, PhD, PMP, LLB, CLE
Principal Consultant, DPO Caribbean
services@dpocaribbean.com

ACKNOWLEDGEMENTS

We wish to thank the Jamaica Cyber Incident Response Team (JaCIRT), particularly Lt. Col. (Ret'd) Godphey Sterling, for their kind assistance in providing invaluable data to facilitate this report.

Please cite this publication as:
DPO Caribbean (2026), *Jamaica Cyber Threat Landscape 201-2025: Roadmap to Resilience*, DPO Caribbean, Jamaica

ISBN 978 976 97440 2 8

TABLE OF CONTENTS

Table of Figures

List of Tables

EXECUTIVE SUMMARY

Cyber threats in Jamaica are increasingly diverse and complex, spanning traditional technical vectors such as ransomware and malware to people-centred attacks, including fraud, social engineering, and identity compromise. Rising internet adoption and digitalisation have expanded the attack surface, making incident reporting and threat visibility essential for national cyber resilience. Studies continue to show that economic and societal consequences extend beyond direct financial loss, affecting trust in digital systems, privacy, and public confidence in institutions.

This report provides a comprehensive analysis of cybersecurity incidents in Jamaica between 2021 and 2025, highlighting trends, victimisation patterns, and sectoral impacts to inform evidence-based national cyber governance. The analysis situates Jamaica within the global and regional cyber threat landscape, emphasising the growing sophistication, diversity, and reach of cybercrime and breaches. It emphasises the importance of systematic incident reporting for understanding risk exposure, identifying vulnerable populations, and guiding evidence-based policy and governance interventions.

The report finds that current reporting mechanisms are functional but likely underutilised due to factors such as reputational concerns and other perceived negative consequences. Importantly, trust, confidentiality, and clarity of legal obligations are critical enablers for improved reporting. Alignment with global practices, including anonymisation, safe-harbour provisions, and clear reporting thresholds, is therefore essential in strengthening participation and capturing a more complete picture of the country's threat landscape.

The report draws on national CIRT data and applies a recognised incident classification framework to categorise incidents (see figure 1). Data analysis covers public, private, and individual groups, with demographic disaggregation highlighting gendered patterns of victimisation. International norms and reporting practices were also considered to ensure comparability and reliability of findings. The analysis spotlights the following:

- **Fraud is the most prevalent incident** category across all years, showing a sharp and sustained increase from 2023 to 2025. This reflects the growing scale of financially motivated cybercrime, particularly scams, impersonation, and fraudulent activity targeting individuals.
- **Abusive Content represents the second largest category**, with consistent growth over time, highlighting rising exposure to harmful, criminal, and harassing online behaviour, and reinforcing the social and psychological dimensions of cyber risk.
- **Information Gathering incidents** (e.g., phishing and social engineering) **show a steady upward trend**, underscoring their role as key enablers of fraud, account compromise, and ransomware.
- **Intrusions and Information Content Security incidents remain comparatively lower in volume** but demonstrate a gradual increase, signalling growing risks related to unauthorised access and data exposure, particularly for organisations.
- **Malicious Code incidents**, including ransomware, increase modestly overall, **with notable growth** in later years, reflecting high-impact but lower-frequency threats that disproportionately affect organisational resilience.
- **Vulnerable Systems incidents are consistently low**, which may indicate underreporting or limited detection, rather than an absence of underlying vulnerabilities.
- **The "Other" category shows a visible rise**, particularly from 2024 onward, suggesting the emergence of new or hybrid incident types and reinforcing the need for ongoing taxonomy refinement.

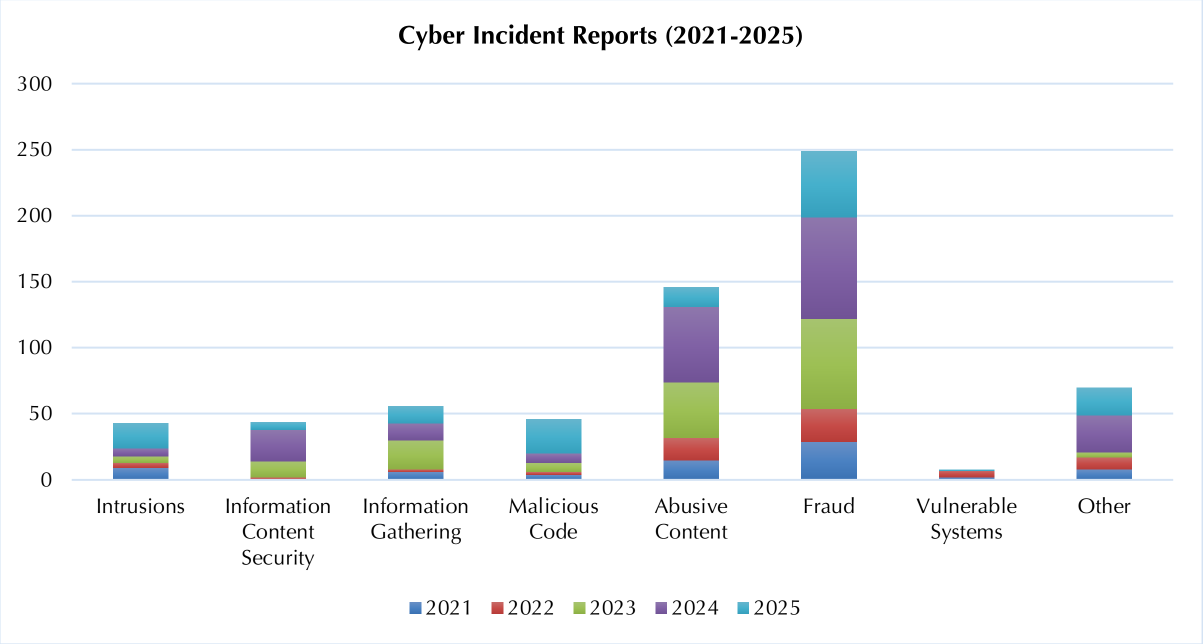


FIGURE 1: CYBER INCIDENTS REPORTED IN JAMAICA (2021-2025)

Individuals consistently account for the majority of incidents, with women disproportionately affected, particularly in cases of fraud, online scams, harmful content, and social engineering attacks. Public organisations report higher incident volumes than private organisations, though the private sector's exposure is rising, driven primarily by ransomware, data compromise, and fraud. Top incidents for organisations include ransomware, social engineering, fraudulent activity, data compromise, and security misconfigurations, while for individuals, the leading threats are fraud, harmful content, social engineering, social media compromise, and misuse of personal information. Across both individuals and organisations, social engineering and ransomware emerge as recurring high-impact vectors, highlighting the interplay between human behaviour and technological vulnerabilities.

Key trends and insights are emphasised as follows:

- **Social engineering is a critical enabling vector**, affecting both individuals and organisations across multiple incident types.
- **Ransomware remains a high-impact threat** for organisations, with potential operational, financial, and reputational consequences.
- **Harmful content and cyber harassment disproportionately affect individuals**, highlighting the social and psychological dimensions of cyber risk.
- **Underreporting persists**, particularly in emerging incident categories and among vulnerable populations, limiting visibility for policymakers.
- **Gendered analysis underscores the need for** targeted awareness, training, and protective measures to address differential risk exposure.

The report recommends a multi-dimensional, evidence-based approach to national cyber governance:

- **Institutionalise a risk-based national cyber incident framework** to standardise reporting and enhance trend analysis.
- **Strengthen reporting incentives** through trust, confidentiality, and legal clarity, particularly for SMEs and individuals.

- **Treat cyber-enabled fraud as a national economic and consumer protection priority**, coordinating across law enforcement, regulators, and industry.
- **Prioritise human-centric cyber resilience**, embedding cyber hygiene, awareness, and social engineering resistance into training and education.
- **Enhance preparedness for high-impact, low-frequency incidents**, including ransomware, data compromise, and infrastructure disruption.
- **Integrate cyber incident reporting** with data protection and privacy governance to harmonise processes and reduce compliance confusion.
- **Leverage incident data as a strategic policy input**, informing risk assessments, resource allocation, legislative reform, and cross-sector collaboration.

The report further spotlights that cyber incidents in Jamaica are not solely technical but systemic, people-centred, and economically consequential, necessitating integrated approaches that combine technical safeguards, public awareness, and cross-sector collaboration. Effective national cyber governance requires technology, trust, institutional coordination, and continuous evidence-based policy design. Building capacity, enhancing reporting, and fostering cross-sector cooperation are therefore essential to strengthening resilience in an evolving threat landscape.

INTRODUCTION

Digital transformation has become a central pillar of economic development, public service delivery, and social inclusion. Governments increasingly rely on digital platforms to deliver essential services, manage public finances, and engage citizens. At the same time, businesses and individuals depend on online systems for commerce, communication, and access to information. This growing digital reliance has spotlighted the "dark side of technology" and significantly expanded national exposure to cyber risks, making cyber incidents a persistent governance and development challenge, extending it beyond a purely technical issue.

Globally, cyber incidents, data breaches and cybercrime continue to evolve in scale, sophistication, and impact. International reporting by entities such as the FBI, ENISA, and UK authorities highlights a steady increase in such incidents, particularly phishing, online fraud, ransomware, and data breaches, affecting both public and private sectors. These incidents generate substantial financial losses, disrupt critical services, and undermine trust in digital systems. Importantly, global evidence shows that cyber incidents disproportionately affect individuals, small businesses, and public institutions with limited cybersecurity capacity, patterns that are especially relevant for developing economies and small states such as Jamaica.

According to the most recent FBI Internet Crime Report[1], the United States alone recorded over 859,000 complaints of suspected internet crime in 2024, with reported financial losses exceeding $16.6 billion, marking a substantial increase in both the scope and economic damage of cyber-enabled crime compared to previous years. Meanwhile, the latest UK Cyber Security Breaches Survey[2] reveals that a significant proportion of organisations (about half of businesses and nearly one-third of charities) experienced some form of cyber breach in the preceding 12 months, with phishing attacks overwhelmingly prevalent, with average incident costs rising across sectors. Comparably, the top five targeted sectors in the EU include public administration (38.2%), transport (7.5%), digital infrastructure and services (4.8%), finance (4.5%) and manufacturing (2.9%), according to The ENISA Threat Landscape 2025 Report[3].

In the Caribbean and other small economies, digitalisation is advancing rapidly, often outpacing institutional and regulatory capacity for managing cyber risks. Jamaica exemplifies this dynamic. National initiatives to expand e-government services, digital financial inclusion, and online commerce have accelerated connectivity and innovation, while simultaneously increasing exposure to cyber threats similar to those observed globally. Despite this growing risk, policy discussions on cybersecurity in Jamaica, and in many comparable contexts, remain constrained by limited empirical evidence on the nature, scale, and impact of cyber incidents at the national level.

A key policy challenge lies in the availability and use of cyber incident data. Cyber incidents are widely underreported due to reputational concerns, lack of awareness, unclear reporting obligations, and limited incentives for disclosure. Where incidents are reported, data are often fragmented or inconsistently classified, limiting their usefulness for policy and risk management. Scientific and policy-based studies have repeatedly emphasised that effective cyber governance depends on reliable incident data to inform risk assessments, prioritise investments, and monitor policy effectiveness.

[1] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf
[2] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
[3] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

National Cyber Incident Response Teams (CIRTs) such as the Jamaica CIRT (JaCIRT) play a pivotal role in monitoring, aggregating, and responding to incidents, acting as both operational defenders and stewards of national cyber situational awareness. Beyond their operational responsibilities for incident response and coordination, CIRTs serve as central repositories of cyber incident information and as trusted interfaces between government, the private sector, and citizens. These teams also serve as critical nodes for detecting emergent threats, analysing incident patterns, and informing broader cyber governance frameworks, functions that are essential for building cyber resilience as cyber vulnerabilities and threat actors proliferate.

This report adopts a policy-oriented, evidence-informed approach to analysing cyber incidents in Jamaica using administrative data collected by the national CIRT. The analysis examines incident trends, affected sectors, and population groups to inform strategic decision-making. The report situates Jamaica's experience within broader global and regional threat landscapes, drawing comparisons with international reporting to identify common risk patterns as well as context-specific challenges.

Based on the foregoing, the central focus of this report is to support improved cyber risk governance by addressing four policy-relevant questions:

1. **What types of cyber incidents are being reported nationally, and how are these evolving over time?**
2. **Which sectors and population groups are most affected, and what does this imply for risk prioritisation?**
3. **How can the national CIRT data be better leveraged to strengthen cyber resilience, improve reporting practices, and inform governance frameworks?**

The importance of this analysis lies in its potential to strengthen evidence-based policymaking. By translating incident-level data into strategic insights, the report supports government authorities in identifying priority risks, targeting awareness and capacity-building initiatives, and aligning national cybersecurity efforts with international best practices. This approach is consistent with global good practices that emphasise risk-based governance, proportional regulation, and cross-sector collaboration.

The contribution of the report is threefold. First, it emphasises how national CIRT data can be operationalised as a strategic policy resource rather than solely an operational tool. Second, it provides one of the first consolidated, evidence-based assessments of Jamaica's cyber incident landscape, addressing a critical information gap for policymakers. Third, it offers policy-relevant insights and recommendations applicable not only to Jamaica but also to other small states and developing economies seeking to strengthen cyber governance in line with global standards.

STRATEGIC CONTEXT AND CONSIDERATIONS

THE GLOBAL AND REGIONAL CYBER THREAT LANDSCAPE

Cyber incidents are increasingly recognised as a strategic governance challenge globally. Ransomware, phishing, malware, and data breaches remain the most common incidents affecting public and private sectors[4]. SMEs and individuals continue to be disproportionately impacted with losses exceeding US$10 billion in the US alone, precipitated by over 3 million complaints in 2024[5]. Similarly, in the United Kingdom, one in three businesses experiences a cyber incident each year, with increasing sophistication and hybrid attack techniques[6].

These global experiences collectively underscore several policy-relevant trends:

1. Cyber incidents are growing in frequency and complexity, affecting both individuals and institutions.
2. Threat actors exploit technical vulnerabilities and human behaviours, making risk management a socio-technical challenge.
3. SMEs and individuals face greater vulnerability, reflecting gaps in awareness, resources, and protective measures.

For small states and developing economies like Jamaica, these trends are particularly important. Rapid digitalisation has increased exposure across sectors and population groups, while resources, governance structures, and incident reporting mechanisms may lag behind threat evolution, creating heightened systemic risk[7].

CYBER GOVERNANCE AND POLICY FRAMEWORKS

Effective cyber governance requires a multi-dimensional, evidence-based approach that integrates technical, legal, regulatory, and institutional measures[8]. Key principles highlighted generally include:

- **Risk-based prioritisation**: Allocate resources to high-impact threats and vulnerable sectors.
- **Incident-informed decision-making**: Use CIRT data to identify trends, evaluate policy effectiveness, and guide cyber resilience investments.
- **Capacity building**: Strengthen national institutions, private sector capabilities, and citizen awareness through coordinated and targeted initiatives.
- **Regulatory alignment**: Ensure laws, policies, and standards support reporting, response, and risk management without imposing disproportionate burdens.
- **Public–private collaboration**: Cybersecurity is a shared responsibility requiring partnerships across sectors.

[4] ENISA Threat Landscape Report 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[5] FBI 2024 Internet Crime Report, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[6] UK Cyber Security Breaches Survey 2024, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

[7] Donalds, C., Barclay, C., & Osei-Bryson, K. M. (2022). Cybercrime and Cybersecurity in the Global South: Concepts, Strategies and Frameworks for Greater Resilience. Routledge

[8] Barclay, C. (2014, June). Sustainable Security Advantage in a Changing Environment: The Cybersecurity Capability Maturity Model (CM 2). In Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world-Impossible without standards? (pp. 275-282). IEEE.

Empirical evidence demonstrates that countries with structured reporting, robust CIRTs, and integrated governance frameworks experience better resilience outcomes and more informed policy decisions[9].

THE IMPORTANCE OF INCIDENT REPORTING

National Cyber Incident Response Teams (CIRTs) are central to effective cyber governance. They collect, analyse, and respond to cyber incidents, acting as critical interfaces between government, private sector, and citizens. Local and global insights underscore that reliable incident reporting enables evidence-based risk assessment, strategic prioritisation, and the development of targeted policy interventions.

However, persistent challenges exist, especially in small developing states like Jamaica[10], such as:

- **Underreporting**: Organisations may avoid reporting incidents due to reputational concerns or regulatory fears.
- **Fragmented data**: Fragmented incident data due to factors such as disconnected systems and the lack of standardised taxonomies reduces its usefulness for operational decision-making, policy analysis, and research.
- **Limited sectoral coverage**: Individuals, SMEs, and public institutions often report inconsistently, creating governance blind spots.
- **Limited empirical research**: Gaps in high-quality data constrain rigorous empirical analysis and evidence-based cybersecurity research.

An important consideration is aligning incident reporting with international frameworks, as standardised classification enables trend analysis, cross-sector comparisons, and benchmarking against global threat landscapes, providing actionable insights for national policy and cyber risk management.

RISK EXPOSURE AND VICTIMISATION PATTERNS

Cyber victimisation analysis shows that risks tend to be unevenly distributed across sectors and populations, where certain groups are more susceptible to certain risks. For example:

- **Individuals**: Individuals are frequently targeted through phishing, identity theft, and online fraud. The extent of risk exposure is largely influenced by digital literacy, online routines, and awareness of preventative and protective measures.
- **Private sector organisations**: SMEs are particularly vulnerable due to limited cybersecurity resources, lack of formalised policies, and relatively weaker incident response capacity.
- **Public institutions**: Government entities remain a high-value target for ransomware and data breaches, with potential impacts on public service continuity, critical infrastructure resilience, and public trust.

Undoubtedly, understanding victimisation patterns is essential for prioritising risk mitigation measures, allocating scarce resources, and tailoring awareness campaigns. Incident data also allow for demographic analyses (e.g., male vs. female users), which can guide targeted interventions to strengthen inclusivity in cybersecurity policies.

[9] ITU Global Cybersecurity Index 2024, https://www.itu.int/epublications/zh/publication/global-cybersecurity-index-2024

[10] Donalds, C., Barclay, C., & Osei-Bryson, K. M. (2022). Cybercrime and Cybersecurity in the Global South: Concepts, Strategies and Frameworks for Greater Resilience. Routledge

ECONOMIC AND SOCIETAL IMPLICATIONS

Cyber incidents carry financial, operational, and societal costs, even when precise losses are underreported. Global estimates indicate billions of dollars in direct and indirect losses from fraud, ransomware, and service disruption[11].

Beyond monetary losses, cyber incidents can:

- Disrupt essential public services and compromise citizen trust.
- Erode business confidence and slow the adoption of digital services.
- Amplify social and psychological impacts, particularly for victims of identity theft or online fraud.

For small economies like Jamaica, these impacts are magnified due to the concentration of critical services, the relative size of national markets, and limited institutional resilience. To this end, risk-informed governance frameworks are essential in mitigating these impacts, including cyber hygiene campaigns, resilience planning, and sector-specific safeguards.

INFORMED POLICY THROUGH INCIDENT DATA

Cyber incidents are a systemic risk with financial, operational, and societal dimensions. While international reports provide high-level evidence and good practices, there is a critical gap in country-specific, incident-based analysis for Caribbean countries like Jamaica.

Currently, national policymakers face challenges, such as:

- Limited empirical evidence on incident types, sectoral impacts, and victimisation patterns.
- Inconsistent reporting and fragmented datasets, which reduce policy design and effectiveness.
- Difficulty linking incident trends to governance and resilience measures.

This report addresses these gaps by analysing administrative data from Jamaica's national CIRT, using internationally recognised classification standards to:

- Identify national incident trends and affected sectors.
- Assess risk exposure and victimisation patterns.
- Draw policy-relevant insights to inform cyber governance, resilience planning, and targeted interventions.

[11] IBM Cost of Data Breach Report 2025, https://www.ibm.com/reports/data-breach

METHODOLOGY

This report adopts a data-driven, policy-oriented approach to analyse cyber incidents reported in Jamaica between 2021 and 2025, with the primary objective of generating insights for the local threat landscape, risk management, victimisation analysis, and national cyber governance.

DATA SOURCE

The primary dataset comprises records from JaCIRT, which collects, categorises, and maintains incident reports submitted by public institutions, private sector organisations, and individuals. The dataset includes information on:

- Period of incident reporting (year)
- Type of incident (e.g., phishing, ransomware, malware, fraud, data compromise)
- Affected groups (public, private, individual)
- Demographic attributes where available (e.g., individual vs. organisational, gender)

While recognising limitations concerning underreporting and potential gaps in completeness, these records represent the most comprehensive national source of cyber incident data available and are consistent with international practices for evidence-based cyber governance.

CLASSIFICATION FRAMEWORK

A cybersecurity classification taxonomy is a structured framework used to categorise and describe different types of security incidents, threats, and policy violations in a consistent and understandable way. Its purpose is to help identify, assess, respond to, and report cybersecurity events by grouping them based on their nature, impact, and method of occurrence.

The research relies on a dual incident classification lens, which includes the local taxonomy adopted by JaCIRT, and the ecsirt.net taxonomy[12] recognised by global CIRTs:

- The local taxonomy provides categories of incidents that span technical, human, physical, and compliance-related incidents, covering areas such as device loss, account compromise, fraud, malware (including ransomware), unauthorised access, misuse of information, and online harms like scams, harassment, and impersonation. The taxonomy is intended to support effective incident response, risk management, regulatory reporting, trend analysis, and communication across technical teams, leadership, and non-technical stakeholders.
- The ecsirt.net taxonomy provides a standardised framework for classifying cyber incident types used by a number of Computer Security Incident Response Teams (CSIRTs/CIRTs) across Europe and internationally[13]. The taxonomy supports consistent incident reporting, analysis, and information sharing across organisations and jurisdictions.
- Using a dual incident reporting classification, combining the national scheme with a standard such as ecsirt.net, provides analytical rigour. Together, they broaden analytical perspectives and enhance the ability to identify patterns and emerging threats, while retaining clear operational relevance.

[12] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

[13] ENISA Good Practice Guide for Incident Management, https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

CYBER INCIDENT REPORTING IN JAMAICA

CURRENT INCIDENT REPORTING PROCESS

A cyber incident typically includes any event that compromises, or may compromise, the confidentiality, integrity, or availability of information systems, networks, or data, such as unauthorised access, malware or ransomware attacks, data breaches, online fraud, service disruption, or cyber harassment[14].

Cyber incident reporting is a structured process designed to enable individuals, private and public institutions to report cybersecurity incidents in a clear, consistent, and efficient manner. This further supports timely incident assessment and response, protects critical infrastructure, prevents further harm, and strengthens national cybersecurity defences.

To this end, incident reporting may be viewed as a critical component of both national cyber resilience and legal compliance.

Any individual or institution that experiences or suspects a cybersecurity incident can report it by visiting the national CIRT website and selecting the "Report a Cyber Incident" link[15]. The online reporting form guides users/reporters step-by-step through the submission process, allowing incidents to be reported securely and efficiently. By completing the form, reporters provide essential information that enables a timely assessment, response, and coordination, while contributing to national efforts to strengthen cybersecurity and mitigate future risks.

The reporting process is organised around five main categories of information.

- **Contact Information**. This information is collected first to identify whether the reporter is the impacted user or acting on behalf of an affected individual or organisation, and to enable follow-up and coordination.
- **Incident Information**. This section captures what happened, who or what was affected, how and when the incident was detected, where it occurred (physical or virtual environment), and how it was discovered, using standardised options that support national analysis and international comparability.
- **Impact Details**. This section documents the consequences of the incident, including whether confidentiality, integrity, or availability were affected, the functional impact on operations, the number of systems and users impacted, and the types of systems involved (such as workstations, servers, networks, cloud services, or critical systems). This section may also include information on data breaches, affected records, recovery status, and containment actions taken.
- **Indicators and Defensive Measures**. This section captures technical and operational details such as indicators of compromise, known vulnerabilities, observed malicious activity, and steps taken to mitigate or contain the incident, which support both immediate response and broader threat intelligence efforts. The Complete stage confirms submission and allows reporters to provide any additional contextual information or request assistance from the national CIRT.

According to JaCIRT, the information provided is used solely for assessing incidents, coordinating appropriate response actions, and, where necessary, sharing anonymised threat intelligence to reduce future risk. They note that submitting the incident reporting form does not replace legal or regulatory

[14] https://www.cirt.gov.jm/
[15] https://www.cirt.gov.jm/form/report-an-incident

obligations, such as the relevant mandatory reporting under the Jamaica Data Protection Act (DPA). Under the DPA, organisations are required to report certain personal data breaches to the relevant authority within 72 hours and to notify affected individuals where required.

GLOBAL NORMS AND PROCESS ALIGNMENT

Jamaica's cyber incident reporting process provides a solid foundation for both operational response and policy-driven cyber risk management.

The incident reporting process *appears to be* closely align*ed* with systems used by *international counterparts, such as* CISA (USA), the UK's NCSC, and European national CSIRTs coordinated through ENISA. *These systems* rely on web-based reporting portals that guide reporters through staged sections covering contact details, incident description, impact assessment, and technical indicators. The use of standard elements such as incident timelines, detection methods, system types affected, and CIA impacts mirrors the data collected in the US CISA Incident Reporting Forms, the UK NCSC's "Report a Cyber Incident" service, and ENISA-aligned national CSIRT templates across EU Member States.

The reporting process comprises detailed impact metrics (number of systems and users affected), system typologies (IT, cloud, ICS, email, IoT), operating systems, CVE identifiers, and stages of observed attacker activity is on par with, and in some cases more granular than, public-facing reporting mechanisms in the other jurisdictions This level of detail supports robust trend analysis, victimology studies, and cyber risk assessments, consistent with international reporting standards. The explicit capture of indicators of compromise and defensive measures also aligns strongly with US and European threat intelligence sharing practices.

Where differences are most apparent is in the legal and regulatory context. In the USA, certain sectors are subject to mandatory reporting requirements under laws such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), with defined timelines and enforcement mechanisms. In the EU, mandatory reporting is embedded in binding frameworks such as NIS2 and the GDPR, with clear obligations and penalties across Member States. The UK similarly imposes statutory reporting duties on regulated entities under the UK GDPR and NIS Regulations. In Jamaica, while the Data Protection Act imposes reporting obligations for personal data breaches, broader mandatory cyber incident reporting across critical sectors is more limited, meaning participation relies more heavily on voluntary compliance and awareness.

Jamaica faces common limitations, including underreporting, uneven awareness among individuals and small businesses, and incomplete information at the time of reporting. However, the structured design of the reporting process places Jamaica in a strong position to progressively improve data quality, expand regulatory coverage, and integrate reporting more deeply into national cyber resilience and governance frameworks.

TRUST AS A KEY ENABLER IN REPORTING CYBER INCIDENTS

An important consideration in the effectiveness of cyber incident reporting systems is trust in how reported information is handled. International evidence consistently shows that reporting rates are strongly influenced by confidence that sensitive information will be treated confidentially, proportionately, and responsibly. Concerns about reputational damage, regulatory exposure, or legal liability can discourage organisations, particularly small and medium-sized enterprises (SMEs), and individuals from reporting incidents, even when clear reporting mechanisms exist.

Within this context, the emphasis on confidentiality, anonymisation, and non-punitive handling of incident data is critical. National CIRTs that clearly communicate how information will be protected, how personal or organisational identifiers will be minimised in shared outputs, and how reports are used primarily for risk mitigation rather than enforcement tend to achieve higher levels of voluntary reporting. This approach supports a cooperative rather than adversarial reporting culture, which is especially important in jurisdictions where mandatory reporting obligations are limited or sector-specific.

For Jamaica, embedding these trust-building principles into the incident reporting process enhances its alignment with global good practice and strengthens participation by individuals and SMEs, who account for a significant proportion of reported incidents. Clear assurances regarding data use, safeguards, and the separation between incident response and regulatory enforcement can help improve data completeness and representativeness. In turn, this supports more accurate national cyber risk assessments and more effective policy interventions, reinforcing the role of incident reporting as a cornerstone of inclusive and resilient cyber governance.

CYBER INCIDENT TRENDS

OVERVIEW

The analysis draws on administrative data comprising cyber incidents reported to or handled by the national CIRT, including notifications submitted by public organisations, private sector entities, and individual users. Between 2021 and 2025, the national CIRT recorded a diverse and evolving profile of cyber incidents, reflecting both changes in the threat landscape and improvements in national reporting and response capacity. The shift from aggregate incident counts in 2021 to more granular, victim-disaggregated reporting from 2022 onward represents a maturation of national cyber incident reporting capacity.

Adopting a dual classification approach in analysing Jamaica's cyber incidents, the incidents are first *presented* using the national CIRT's operational taxonomy, which reflects local reporting practices and contextual realities (Table 1). These incidents are then mapped to the internationally recognised eCSIRT.net taxonomy, which is aligned with FIRST standards and widely used across national and sectoral CIRTs globally (Table 2).

The five-year incident dataset reveals a clear and sustained growth in reported cyber incidents, rising from 73 incidents in 2021 to a peak of over 200 incidents in 2024, before declining slightly in 2025. This trend aligns with international observations reported by law enforcement and cybersecurity agencies, which note both an increase in cyber activity and improvements in reporting mechanisms, rather than a linear increase in attacks alone.

When analysed through the eCSIRT.net taxonomy, the incident data reveal a clear evolution from predominantly technical and content-related incidents in 2021 toward increasingly human-centric and economically motivated cybercrime by 2024 - 2025. The taxonomy-based view highlights that cyber risk in Jamaica is not monolithic. The categories of incidents span social harms (abusive content), financial crime (fraud and scams), privacy violations (data disclosure), and organisational resilience threats (ransomware and intrusions). This reinforces the need for cross-sectoral governance, rather than purely technical responses.

VICTIMOLOGY

Individuals represent the majority of victims each year, far outnumbering public and private organisations combined. This aligns with global observations that individuals are frequently targeted by scams, harassment, and identity-related crimes. Public organisations show a lower but steady rate of reported incidents, particularly ransomware and social engineering, emphasising targeted attacks on government infrastructure.

INDIVIDUALS AS PRIMARY VICTIMS

Individuals account for the majority of reported cyber incidents, notably in online scams, harassment, social engineering, and harmful content. This reflects their vulnerability, partly due to lower cybersecurity awareness and protective measures compared to organisations, and highlights a citizen-facing cyber risk profile, where everyday digital interactions, messaging, e-commerce, and social platforms serve as primary attack surfaces.

Gender Disparities in Cyber Victimisation

Female victims consistently outnumber males across most incident categories, especially in cyber harassment, harmful content, and social engineering. This suggests gendered patterns in victimisation and emphasises the need for gender-sensitive approaches in cyber policy and support frameworks.

This aligns with research indicating that women are more likely to experience cyber-enabled harassment and reputational harm, while men may be more affected by certain financial fraud schemes. These findings have implications for gender-sensitive cyber policy, victim support services, and public awareness campaigns.

Sectoral Insights: Public vs Private Exposure

While individuals dominate numerically, public and private organisations face more complex and potentially systemic risks, particularly in:

- Ransomware
- Data compromise
- Social engineering
- Vulnerability disclosures

Notably, ransomware incidents increasingly affect public and private organisations, with a marked rise in 2024–2025. Although fewer in number than individual-focused scams, these incidents carry disproportionate economic and operational consequences, including service disruption, reputational damage, and recovery costs. These findings spotlight critical vulnerabilities in business cybersecurity practices and the need for enhanced resilience measures.

From a technical perspective, patch management and configuration controls, incident response preparedness, sector-specific intelligence sharing and other measures are critical practices.

CYBER INCIDENTS IN FOCUS (2021-2025)

The incident data shows a clear evolution in the local cyber threat landscape, marked by a broader mix of economically motivated, socially exploitative, and human-centric risks, as well as improved reporting maturity.

In 2021, incidents were largely concentrated in traditional categories such as fraud, identity theft, phishing, and unauthorised access, with comparatively low volumes.

From 2022 onward, the introduction and growth of categories including cyber harassment, social engineering, account compromise, and vulnerability disclosures signal both expanding threat vectors and more refined classification.

2023 and 2024 represent a period of escalation, with sharp increases in incident volume driven by fraudulent activity, harmful or criminal content, ransomware, misuse of personal information, and social engineering, culminating in a peak in 2024. The emergence of data compromise, service disruption, and system intrusion further points to increasing organisational exposure.

Although total incidents declined in 2025, elevated levels of ransomware, online scams and impersonation, social media compromise, and residual "Other" incidents indicate a continued concentration of high-impact and financially driven threats, rather than a reduction in overall risk.

Collectively, these trends reinforce the need for risk-based classification, human-focused mitigation strategies, and sustained investment in detection and reporting capabilities.

TABLE 1: REPORTED CYBER INCIDENTS BY TYPE AND YEAR (2021–2025)

#	Incident Type	2021	2022	2023	2024	2025
1.	Account Compromise	-	1	-	-	-
2.	Availability-Sabotage	3	-	-	-	-
3.	Cyber Harassment	-	11	2	-	4
4.	Data Compromise	-	2	-	16	6
5.	Defacement	3	-	-	-	-
6.	Denial of Service (DoS)/Service Disruption	-	-	-	1	-
7.	Fraud/Fraudulent Activity	17	25	68	77	8
8.	Harmful/Criminal Content	15	6	40	57	11
9.	Identity Theft	12	-	-	-	-
10.	Malware	2	1	-	1	4
11.	Misuse of Personal Information	-	-	12	8	-
12.	Online Scams/Impersonation	-	-	-	-	42
13.	Phishing	6	-	-	-	-
14.	Potential Device Compromise	-	-	-	-	3
15.	Ransomware	2	1	7	6	19
16.	Security Misconfigurations	-	-	-	-	1
17.	Social Engineering	-	2	22	13	13
18.	Social Media Compromise	-	1	3	-	16
19.	Spam	2	-	-	-	-
20.	System or Network Intrusion	-	-	-	1	-
21.	Unauthorised Access	-	2	2	5	3
22.	Unauthorised Access to Information	7	-	-	-	-
23.	Unauthorised Modification of Information	2	-	-	-	-
24.	Vulnerability Disclosures	-	5	-	-	-
25.	Vulnerable Systems	2	-	-	-	-
26.	Other	-	9	4	27	21
	TOTAL	**73**	**66**	**160**	**212**	**151**

Table 2 and Figure 2 present a consolidated view of national cyber incident data mapped to the CSIRT.net primary taxonomy, while retaining the original incident classifications to ensure transparency and accuracy. The mapping demonstrates a clear concentration of incidents within Fraud, Abusive Content, and Malicious Code categories, reflecting the growing prevalence of financially motivated and people-centred cyber threats. At the same time, the inclusion of Intrusions and Information Content Security highlights increasing exposure to unauthorised access and data-related risks, particularly for organisations. The persistence and growth of the "Other" category further indicates the emergence of new or hybrid incident types, reinforcing the need for ongoing taxonomy review and adaptive cyber risk governance.

TABLE 2: CYBER INCIDENTS MAPPED TO CSIRT.NET TAXONOMY (2021–2025)

CSIRT.net Primary Category	JaCIRT Incident Category	2021	2022	2023	2024	2025
1. Intrusions	Social Media Compromise, Account Compromise, Unauthorised Access, System/Network Intrusion	9	4	5	6	19
2. Information Content Security	Data Compromise, Misuse of Personal Information	-	2	12	24	6
3. Information Gathering	Phishing, Social Engineering	6	2	22	13	13
4. Malicious Code	Malware, Potential Device Compromise, Ransomware	4	2	7	7	26
5. Abusive Content	Harmful/Criminal Content, Cyber Harassment	15	17	42	57	15
6. Fraud	Fraud/Fraudulent Activity, Online Scams, Identity Theft	29	25	68	77	50
7. Vulnerable Systems	Security Misconfigurations, Vulnerability Disclosures, Vulnerable Systems	2	5	-	-	1
8. Other	Availability-Sabotage, Defacement, DoS, Spam, Other	8	9	4	28	21
TOTAL		**73**	**66**	**160**	**212**	**151**

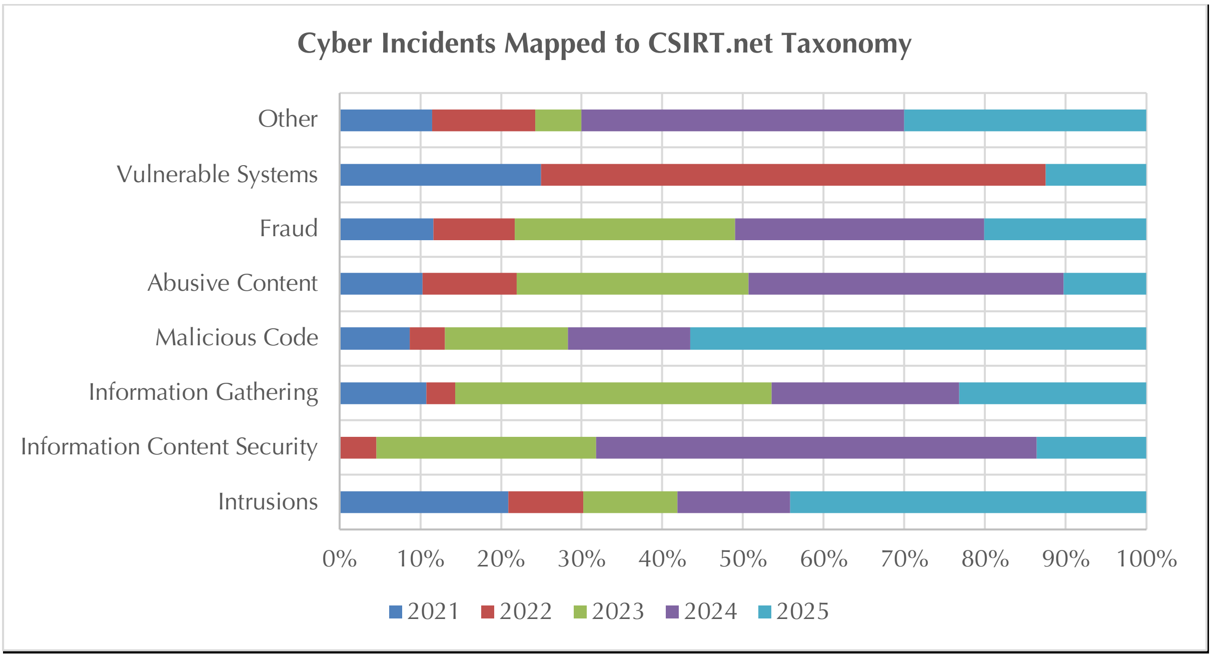


FIGURE 2: CYBER INCIDENTS MAPPED TO CSIRT.NET TAXONOMY (2021–2025)

TOP CYBER INCIDENTS

Insights into the top incidents affecting individuals and organisations are presented (Tables 3 and 4), revealing clear differences in risk exposure, attack vectors, and impact across these groups. Together, these patterns illustrate how cyber risk manifests differently across user groups, reinforcing the need for tailored prevention strategies, reporting mechanisms, and policy responses for individuals and organisations alike.

TABLE 3: TOP 5 INCIDENTS AFFECTING INDIVIDUALS (2022–2025)

Rank	Incident Type
1	Fraudulent Activity / Online Scams / Impersonation
2	Harmful or Criminal Content
3	Social Engineering
4	Social Media Compromise
5	Misuse of Personal Information / Unauthorised Access to Personal Files

Analysis of cybersecurity incidents affecting individuals from 2022 to 2025 reveals several critical insights (Table 3). First, fraudulent activity, online scams, and impersonation constitute the most prevalent threats, accounting for the largest proportion of incidents and reflecting significant economic and personal losses. Second, harmful or criminal content ranks second, demonstrating the growing psychological and reputational risks faced by individuals online. Third, social engineering is a key enabler of attacks, often facilitating fraud, account compromise, and ransomware, highlighting the central role of human behaviour in cyber risk. Fourth, social media compromise continues to be a prominent vector, enabling impersonation, misinformation, and privacy breaches. Finally, misuse of personal information and unauthorised access to personal files underscore the vulnerability of sensitive personal data, with long-term implications for privacy and identity security. Collectively, these findings emphasise that individual cyber risk is people-centred, pervasive, and economically significant, necessitating targeted awareness, digital literacy, and accessible reporting and support mechanisms to enhance resilience.

TABLE 4: TOP 5 INCIDENT TYPES BY ORGANISATION TYPE (2022–2025)

Organisation Type	Top Incident Types
Public Organisations	1. Social Engineering
	2. Ransomware
	3. Fraudulent Activity
	4. Denial of Service / Service Disruption
	5. Security Misconfigurations
Private Organisations	1. Ransomware
	2. Fraudulent Activity
	3. Data Compromise
	4. Unauthorised Access
	5. Social Engineering

Analysis of organisational cybersecurity incidents from 2022 to 2025 highlights several key trends critical for national cyber resilience (Table 4). First, ransomware consistently ranks as the top threat for both public and private organisations, reflecting its high operational and financial impact. Second, social engineering remains a leading vector in public organisations, targeting employees and emphasising the importance of awareness and role-based training. Third, fraudulent activity and data compromise dominate private-sector incidents, illustrating the sector's exposure to financial loss and sensitive information breaches. Fourth, public organisations report a higher overall volume of incidents than private organisations, though the private sector's share is steadily increasing, signalling expanding cyber risk across the economy. Finally, other incident types, such as security misconfigurations, unauthorised access, and service disruption, while less frequent, can have significant consequences, underscoring the need for comprehensive prevention, monitoring, and response strategies. These findings collectively demonstrate that organisational cyber risk is systemic, evolving, and requires proactive, cross-sector mitigation measures, including technical safeguards, staff training, and coordinated incident response.

CYBER INCIDENTS BY KEY DEMOGRAPHICS

From 2022 onward, the introduction of group-based reporting reveals a consistent pattern in which individuals account for the majority of incidents each year, driven largely by fraud, online scams, harmful content, and social engineering. Over the same period, public and private sector incidents increased steadily, reflecting both growing digital exposure and improvements in detection and reporting maturity. Incident volumes peak in 2024 before moderating in 2025, suggesting a combination of heightened threat activity, improved awareness, and evolving reporting behaviours. Overall, the data highlights a transition from predominantly technical concerns to systemic cyber risks that affect individuals, organisations, and national resilience, underscoring the need for integrated, trust-based, and evidence-driven cyber governance.

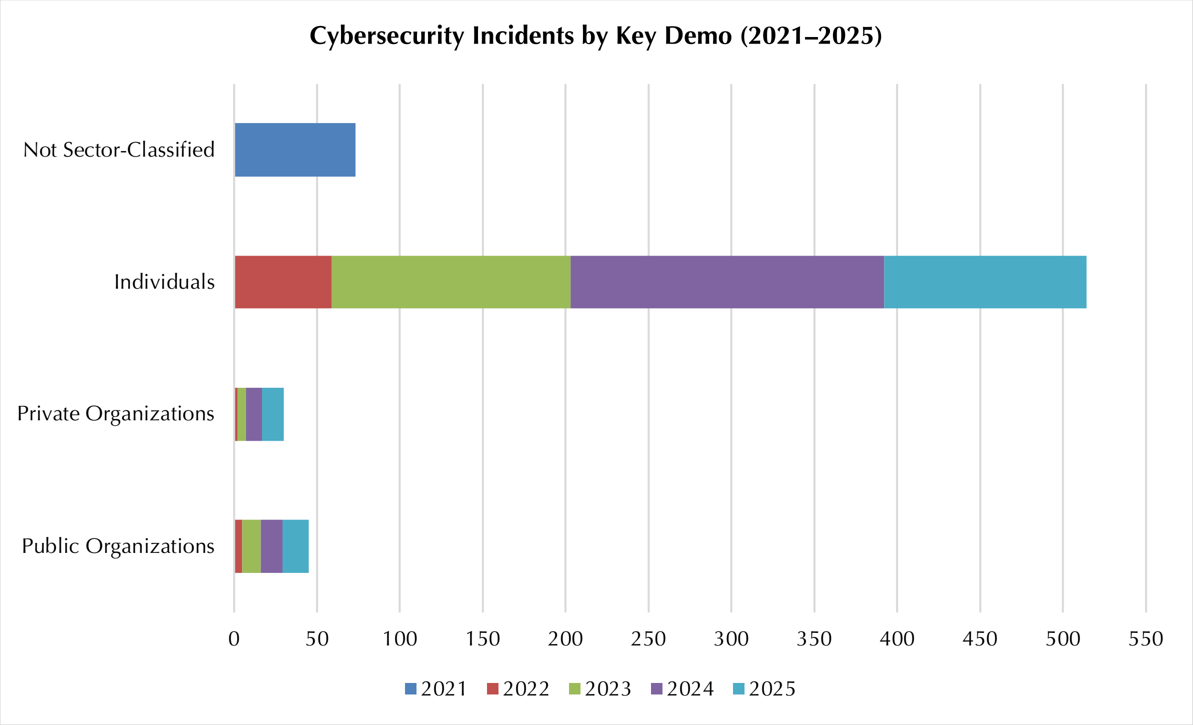


FIGURE 3: CYBER INCIDENTS PER CATEGORY (2021-2025)

Other key insights (Figure 3) include the following:

- Individuals account for the overwhelming majority of reported incidents across the five years, far exceeding public and private organisations combined.
- Incident volumes affecting individuals increase sharply from 2022 onward, peaking in 2024 and remaining high in 2025, reflecting rising exposure to fraud, harmful content, social engineering, and scams as digital adoption expands.
- Public organisations consistently report more incidents than private organisations, suggesting either higher exposure, stronger detection and reporting mechanisms, or greater reporting obligations within the public sector.
- Private sector reporting remains comparatively low, which may indicate underreporting, limited detection capacity among SMEs, or reluctance to report incidents due to reputational or regulatory concerns.
- Overall incident volumes rise steadily over time, with the most pronounced growth occurring between 2023 and 2024, indicating an expanding threat landscape rather than isolated spikes.

INCIDENTS BY GENDER DISTRIBUTION

Between 2021 and 2025, reported cybersecurity incidents demonstrate a pronounced gendered impact, with female victims consistently outnumbering male victims. While 2021 lacks gender-disaggregated data, the four subsequent years reveal that women account for the majority of incidents, ranging from 63% in 2022 to over 89% in 2024, and an overall share of 77.5% across 2022–2025. This disparity is particularly evident in high-volume incident types such as fraud, online scams, harmful or criminal content, social media compromise, and cyber harassment, indicating that women are disproportionately affected by both economic and social cyber risks. Male victims, while lower in number, are more represented in technically complex incidents such as ransomware and social engineering in certain years. The persistent gender imbalance underscores the need for gender-responsive cybersecurity strategies, including awareness campaigns, targeted prevention measures, and victim support mechanisms, to ensure equitable protection in the digital environment.

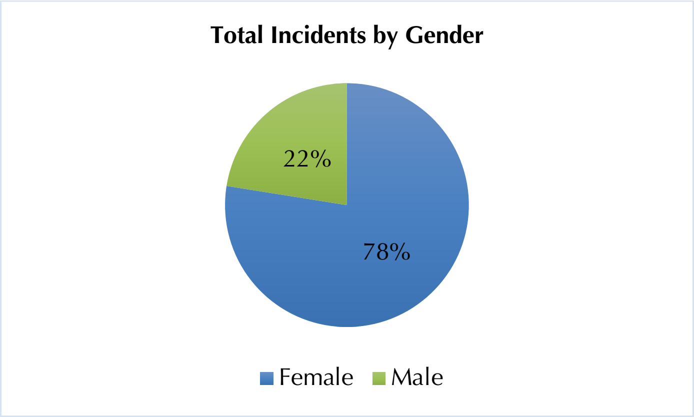


FIGURE 4: INCIDENTS BY GENDER (2022-2025)

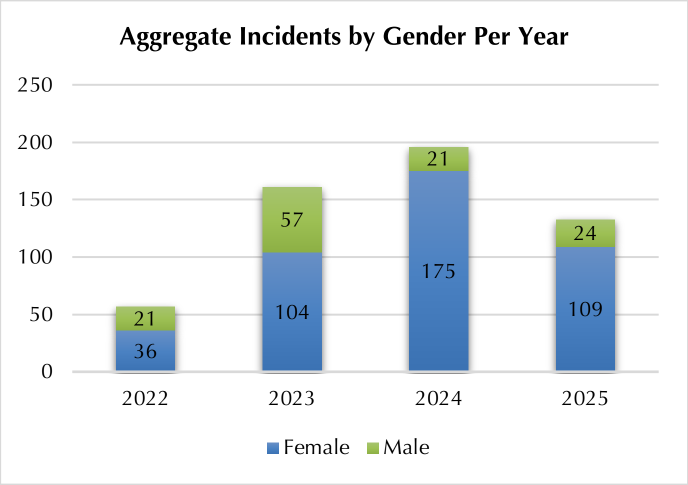


FIGURE 5: AGGREGATE INCIDENTS BY GENDER (2022-2025)

PUBLIC VS PRIVATE SECTOR INCIDENTS

Between 2022 and 2025, reported cyber incidents increased steadily across both sectors, with incidents affecting public organisations accounting for 60% of total organisational incidents, while private organisations comprising 40%. Annual incidents in the public sector more than tripled, rising from 5 in 2022 to 16 in 2025, while the private sector saw a sharper proportional increase, growing from 2 to 13 incidents over the same period. This sustained year-on-year growth reflects an expanding digital attack surface and a shift toward economically motivated and human-centric threats, consistent with global trends. The upward trend also suggests improved detection and reporting maturity, particularly as organisations strengthen their ability to identify and formally report cyber incidents.

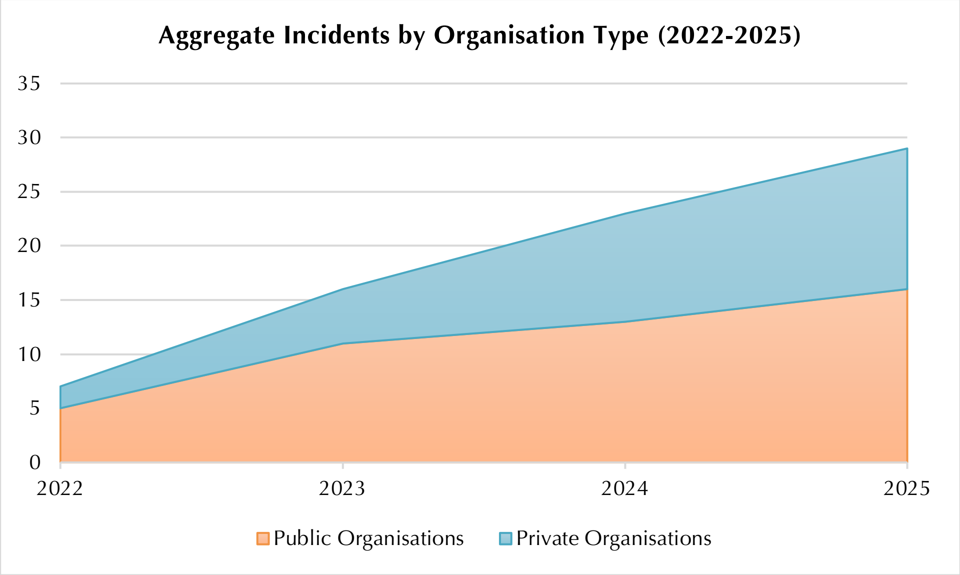


FIGURE 6: AGGREGATE INCIDENTS BY SECTOR (2022-2025)

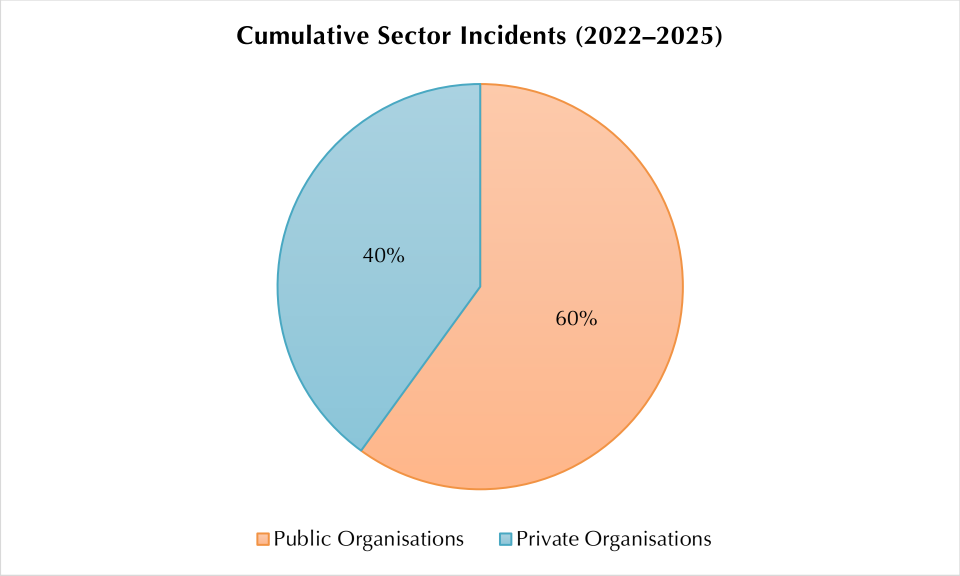


FIGURE 7: SECTOR INCIDENTS (2022-2025)

INSIGHTS FROM INCIDENT TYPES

A critical insight from the dataset is that non-technical threats, such as social engineering, fraud, harmful content, and impersonation, now exceed purely technical incidents, including malware and intrusion-based attacks. This shift has significant governance implications. Cybersecurity can no longer be treated solely as a technical or IT risk; it must be addressed as a cross-sector policy challenge requiring coordinated engagement among the ecosystem, to include law enforcement, financial regulators, digital platforms, and consumer protection authorities. Correspondingly, cyber resilience metrics should evolve beyond traditional indicators such as system availability or uptime to encompass measures of user harm, trust erosion, financial loss, and societal impact.

Other key trends and insights are outlined below.

Harmful Content and Cyber Harassment

The Harmful Content category (including harmful/criminal content and cyber harassment) remains a consistent feature across the period, peaking in 2024. This category disproportionately affects individual users rather than organisations, underscoring the challenges in managing online behaviour and content regulation while spotlighting cyber victimisation as a social and public safety issue.

The fluctuations, high levels in 2021 and 2024, lower levels in 2022 and 2023, likely reflect changes in reporting behaviour, platform moderation dynamics, as well as public awareness and confidence in reporting mechanisms.

These incidents sit at the intersection of cybersecurity, online safety, and criminal justice, requiring coordinated responses involving regulators, law enforcement, and social service agencies.

Fraud and Online Scams

The Fraud category emerges as the most significant and persistent threat, particularly from 2022 onwards. Fraudulent activity shows a strong upward trajectory through 2024, while online scams and impersonation surge dramatically in 2025.

This pattern is consistent with global trends where cyber-enabled fraud accounts for a significant share of reported losses[16]. The data therefore suggest that:

- Cybercrime in Jamaica is increasingly financially motivated
- Individuals are the primary victims
- Technical sophistication is often secondary to deception and trust exploitation

These findings support treating fraud not solely as a cybersecurity issue, but as a national economic and consumer protection concern. The findings also underscore the need to treat cybercrime not only as a technical issue but as a consumer protection, financial crime, and digital literacy challenge.

Identity Theft and Phishing

Identity theft and phishing are prominent in 2021 but largely disappear as standalone categories in subsequent years. This does not imply the disappearance of the threats; rather, it likely suggests conceptual and reporting consolidation.

Later incidents classified as fraud, social engineering, or account compromise often involve phishing and identity theft as enabling mechanisms. This highlights a methodological insight: taxonomy maturity affects apparent trends, and policymakers should therefore interpret declines cautiously.

Account Compromise and Social Media Takeovers

Account compromise, particularly social media compromise, shows a marked increase by 2025. This reflects:

[16] See for example the FBI Internet Crime Report 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

- Increased reliance on digital identity
- Weak authentication practices
- Reuse of credentials across platforms

These incidents reinforce the importance of basic cyber hygiene, such as multi-factor authentication, and point to digital identity protection as a growing policy priority.

Data Disclosure and Misuse of Personal Information

Incidents involving data compromise and misuse of personal information increased markedly in 2023 and 2024. This trend points to persistent shortcomings in data protection and access control measures affecting individuals, private and public organisations. This incident trend aligns with:

- Expansion of data-driven services
- Growing awareness of privacy harms
- Strengthened legal obligations under data protection frameworks

These findings underscore the need for closer alignment between CIRT operations and data protection authorities, particularly around breach notification, impact assessment, and victim redress.

Unauthorised Access and Intrusions

Incidents classified under unauthorised access and intrusions remain relatively low in volume but are strategically significant. The continued occurrences of unauthorised access indicate persistent weaknesses in data security and access control practices, with impacts observed across both private organisations and individual users.

Even small numbers in this category can translate into disproportionate operational and reputational harm, especially for public-sector entities and critical services.

Social Engineering Drives Multiple Risks

The sharp rise in Social Engineering incidents from 2023 onward confirms its role as a foundational threat vector. Rather than standing alone, social engineering enables fraud, ransomware, account compromise, and data disclosure.

This reinforces international policy consensus that human factors are now central to cyber risk, requiring sustained investment in awareness, training, and behavioural interventions.

Malware and Ransomware

While Malware incidents remain modest in number, Ransomware shows a clear upward trend, peaking in 2025, mirroring global threat landscapes where ransomware has become a prime tactic for cybercriminals targeting both organisations and individuals. Consistent with global experience, ransomware is less frequent than scams but far more disruptive and costly.

The data support prioritising ransomware preparedness, even if incident counts appear modest relative to fraud.

Vulnerabilities, DoS, and Defacement

Vulnerability disclosures, DoS incidents, and defacement appear primarily in earlier years. Their decline may reflect improved baseline security, shifts in attacker focus, under-reporting or reclassification.

The findings reinforce the importance of continuous taxonomy review and technical capacity building to ensure detection keeps pace with evolving threats.

"Other" Category

The persistent growth of the unclassified category, especially in 2024 and 2025, signals:

- Emerging or hybrid incident types
- Reporting ambiguity
- Limits of existing classification schemas

From a methodological and policy standpoint, this category is a diagnostic indicator, pointing to areas where the taxonomy and reporting guidance should evolve.

Notable Gaps and Underreporting Risks

Despite rising incident volumes, the data almost certainly reflect only a partial view of the true cyber risk landscape, consistent with international experience where underreporting remains a persistent challenge. Several incident categories appear underrepresented or absent from the national dataset, pointing less to an absence of risk and more to analytical and reporting blind spots. Notably, no incidents were recorded under *Physical Security Breaches* or *Compliance and Regulatory Violations*, despite global regulatory enforcement reaching an estimated US$1 billion in fines in 2025 alone[17]. This disparity suggests that underreporting, potentially reinforced by concerns over mandatory reporting to regulatory authorities, like the Office of the Information Commissioner (OIC), alongside limited classification coverage and insufficient reporting incentives, are more plausible explanations than uniformly strong controls.

A similar pattern is evident in the absence of reported *loss or theft of company-owned devices* and *system failures*, which contrasts sharply with international evidence indicating that compromised or lost endpoints remain a significant driver of security incidents globally[18]. While categories such as *Misuse of Personal Information* and *Unauthorised Access to Personal Files* partially capture privacy-related harms, their growing presence reflects a broader global trend of data exposure and erosion of personal privacy, now affecting a majority of digital users.

Several factors continue to suppress reporting, including fear of reputational damage, uncertainty about what constitutes a reportable incident, limited awareness of reporting mechanisms, and concerns over confidentiality and potential regulatory consequences. Taken together, these gaps underscore the need for ongoing taxonomy refinement, clearer reporting guidance, and better integration of physical, operational, and compliance-related risks into national cyber incident frameworks. International good practice demonstrates that trust-based reporting environments, characterised by anonymisation, non-punitive handling, and transparent communication, are critical to improving reporting rates, particularly among SMEs and individuals, and to strengthening the overall quality of national cyber risk intelligence.

[17] https://www.enforcementtracker.com/?insights
[18] https://www.ibm.com/think/topics/data-breach

KEY INSIGHTS

1. **Cyber risk is increasingly human-centred, not purely technical**
The majority of reported incidents relate to fraud, scams, social engineering, harmful content, and account compromise. This confirms that cyber risk in Jamaica is driven primarily by exploitation of trust, behaviour, and digital identity, rather than advanced technical attacks alone.
2. **Cyber-enabled fraud is the dominant and most persistent threat**
Fraudulent activity and online scams represent the largest share of incidents across the period, mirroring global trends. These incidents disproportionately affect individual users, indicating that cybercrime is now a significant consumer protection and economic policy issue.
3. **Social engineering is a critical enabling vector across incident types**
The sharp increase in social engineering incidents from 2023 onward highlights its role in facilitating fraud, ransomware, account compromise, and data breaches. Addressing cyber risk therefore requires sustained investment in cyber hygiene, awareness, and behavioural resilience.
4. **Ransomware incidents are fewer in number but high in impact**
Although ransomware incidents are less frequent than scams or fraud, their upward trend and disruptive nature justify prioritising preparedness, resilience, and response capabilities, particularly within public institutions and critical services.
5. **Data protection and privacy risks are becoming more visible**
The emergence of data compromise and misuse of personal information incidents in later years reflects growing data exposure and awareness. This underscores the need for closer alignment between cyber incident response and data protection governance.
6. **Account compromise and social media takeovers signal rising digital identity risk**
The increase in account and social media compromises highlights vulnerabilities in authentication practices and identity management, reinforcing the importance of multi-factor authentication and secure credential use.
7. **Low-frequency technical intrusions still pose strategic risk**
Unauthorised access, intrusions, and system-level incidents remain relatively infrequent but carry disproportionate operational and reputational consequences, particularly for public-sector organisations.
8. **The growing "Other" category indicates emerging threats and taxonomy limits**
The expansion of the "Other" category suggests evolving incident types and classification challenges. This highlights the importance of periodic taxonomy review and refinement to maintain analytical clarity.
9. **Improved reporting and classification reflect improved maturity**
The increase in total incidents over time reflects not only rising threat exposure but also greater reporting, awareness, and institutional maturity within the national CIRT framework.
10. **Distrust influences incident reporting**
General distrust influences individuals, private and public entities in reporting incidents, which can be mitigated by managing trust in how data is handled, including any perceived negative consequences of reporting.
11. **eCSIRT.net alignment strengthens policy relevance and international comparability**
Mapping incidents to the eCSIRT.net taxonomy enables meaningful comparison with international datasets and supports evidence-based cyber policy, investment prioritisation, and governance reform.

FIGURE 8: KEY INSIGHTS BOX

POLICY RECOMMENDATIONS

Jamaica's cyber incident landscape from 2021 to 2025 mirrors global trends but with distinct local characteristics, especially the predominance of individual victims and gendered victimisation patterns. Addressing these challenges demands a holistic policy approach integrating awareness, capacity building, regulatory reform, and data-driven governance to enhance national cyber resilience and protect citizens, businesses, and public institutions alike.

Robust cyber governance depends on evidence-based frameworks, trusted reporting, cross-sector collaboration, and sustained investment. Recent empirical insights from the Global Cybersecurity Index (GCI) 2024 Caribbean analysis[19] highlight both progress and persistent gaps in national commitments, reinforcing why strategic policy reform is urgent and timely.

The following recommendations translate incident data and observed trends into actionable policy measures aimed at strengthening cyber resilience, improving reporting, and aligning national practice with global standards.

INSTITUTIONALISE A RISK-BASED NATIONAL CYBER INCIDENT FRAMEWORK

Recommendation
Adopt a formally endorsed, risk-based incident classification framework aligned with international standards, such as eCSIRT.net, and integrate it into national reporting and governance obligations.

Rationale
Caribbean nations' mixed performance in the GCI, with varied rankings across legal, technical, organisational, capacity, and cooperation pillars, underscores inconsistent maturity in cybersecurity governance. A harmonised classification framework improves clarity, supports trend analysis, and strengthens comparability within the region and with international peers.

Proposed Actions

- Mandate a baseline national classification taxonomy across public reporting.
- Enable controlled country-specific extensions while keeping international mapping intact.
- Review taxonomy periodically to respond to emerging threats.

[19] An Analysis of the Global Cybersecurity Index (GCI) 2024: Progress, Challenges and Opportunities for Cybersecurity in the Caribbean, ISBN: 978 976 97440 0 4, https://www.researchgate.net/publication/385417927_An_Analysis_of_the_Global_Cybersecurity_Index_GCI_2024_-_Progress_Challenges_and_Opportunities_for_Cybersecurity_in_the_Caribbean

STRENGTHEN REPORTING INCENTIVES THROUGH TRUST, CONFIDENTIALITY, AND LEGAL CLARITY

Recommendation
Design reporting mechanisms prioritising confidentiality, anonymisation, and non-punitive handling to encourage greater participation, especially among SMEs and individuals.

Rationale
The GCI analysis identifies legal and organisational gaps in many Caribbean countries, contributing to weak reporting cultures and visibility of cyber incidents. This can create concerns about reputation and penalties, especially in contexts where maturity is still evolving, and may discourage voluntary reporting.

Proposed Actions

- Publish clear commitments on data handling and reporting safeguards.
- Separate incident reporting from automatic enforcement where legally feasible.
- Promote “safe harbour” principles for good-faith reporting.

ADDRESS CYBER-ENABLED FRAUD AS A NATIONAL ECONOMIC RISK

Recommendation
Treat cyber-enabled fraud and online scams as strategic national economic and consumer protection concerns, not just cybersecurity issues.

Rationale
The 2024 GCI Caribbean analysis highlights that while legal frameworks may exist, implementation gaps, especially in technical response and organisational measures, leave individuals and consumers exposed. Volume-driven threats like fraud and impersonation thus demand integrated policy responses with economic regulators and consumer protection agencies.

Proposed Actions

- Establish joint tasking between CIRTs, financial regulators, law enforcement, and consumer agencies.
- Improve operational data sharing with financial institutions, telecoms, and platforms.
- Use real incident data to inform public awareness campaigns.

PRIORITISE HUMAN-CENTRIC CYBER RISK MITIGATION

Recommendation
Embed social engineering resistance and cyber hygiene across national resilience strategies.

Rationale
Both GCI performance and observed incident trends emphasise that building technical capacity alone is insufficient. A region with emerging technical maturity still faces fundamental human factors, such as phishing, weak credentials, and social engineering, that amplify risk.

Proposed Actions

- Mandate regular cyber awareness training for public servants.
- Develop SME-tailored guidance on phishing, identity protection, and credential management.
- Integrate cyber awareness into educational curricula and national digital literacy initiatives.

ENHANCE PREPAREDNESS FOR HIGH-IMPACT, LOW-FREQUENCY INCIDENTS

Recommendation
Strengthen readiness for ransomware, major data compromise, and critical infrastructure disruption.

Rationale
The GCI analysis underscores that technical measures and operational readiness often lag behind legal frameworks in Caribbean countries, making them more vulnerable to high-impact disruptions that originate outside routine incident patterns.

Proposed Actions

- Promote resilience fundamentals (offline backups, patching, access control).
- Encourage incident response planning and exercises across sectors.
- Issue sector-specific guidance for ransomware and other high-impact vectors.

IMPROVE DATA PROTECTION AND PRIVACY INCIDENT GOVERNANCE

Recommendation
Link cyber incident reporting more closely with data protection and privacy governance frameworks.

Rationale
GCI findings show that many Caribbean countries score unevenly across legal and organisational pillars, resulting in fragmented governance approaches. Stronger integration enhances clarity around breach notifications and aligns national requirements with privacy norms.

Proposed Actions

- Harmonise JaCIRT and the OIC reporting requirements.
- Clarify thresholds, timelines, and responsibilities for dual reporting.
- Provide practical guidance on navigating overlapping obligations.

REDUCE UNDER-REPORTING THROUGH CAPACITY BUILDING

Recommendation
Invest in national capacity building for detection, reporting, and analysis.

Rationale
Caribbean countries often score higher on legal measures and lower on technical and organisational pillars, suggesting that detection and operational capability gaps hinder both incident response and visibility.

Proposed Actions

- Provide targeted technical assistance to SMEs and public bodies.
- Expand network and endpoint monitoring across sectors.

- Offer accessible reporting options for individuals and small entities.

USE INCIDENT DATA AS A STRATEGIC POLICY INPUT

Recommendation
Formalise the use of incident data in national cyber strategy, risk assessments, and investment decisions.

Rationale
The GCI Caribbean analysis demonstrates that benchmarking against international standards and tracking progress across multiple cybersecurity pillars reveals clear policy blind spots and capacity gaps that warrant focused action.

Proposed Actions

- Publish anonymised national incident trend reports regularly.
- Use data to guide funding prioritisation and legislative reform.
- Benchmark national performance against regional and global peers.

Insights from the GCI 2024 Caribbean analysis reinforce that national cybersecurity maturity is multi-dimensional, requiring legal frameworks, technical capacity, organisational readiness, cooperation mechanisms, and continuous learning across all key stakeholders within the ecosystem.

Cyber incidents in Jamaica and the broader Caribbean reflect systemic, people-centred, and economically consequential risks, not merely isolated technical failures. Effective national cyber governance therefore demands integrative, trust-based, and evidence-aligned policy design, anchored in international good practice and informed by sustained data collection and analysis.

Together, these findings demonstrate that systematically collected, internationally aligned cyber incident data provides actionable intelligence for governance, prevention, and resilience-building. The Jamaican case illustrates how national CIRT administrative data can bridge technical cybersecurity practice, criminological insight, and public policy, particularly in small-state and developing contexts.

FUTURE DIRECTIONS AND EMERGING POLICY QUESTIONS

While this report provides one of the first systematic, taxonomy-aligned analyses of cyber incidents reported to the national CIRT, it also highlights several important areas where further research would substantially deepen policy relevance and analytical precision. Addressing these gaps or opportunities would strengthen evidence-based decision-making and support the continued maturation of national cyber governance.

Future research will focus on quantifying the economic impact of cyber incidents. Although the present analysis demonstrates the prevalence of fraud, scams, and ransomware, it does not estimate direct or indirect financial losses, productivity disruptions, recovery costs, or reputational damage[20]. Developing cost models, drawing on international methodologies used by international organisations such as OECD or World Bank, would allow policymakers to better assess return on investment for cybersecurity initiatives and prioritise interventions based on economic risk rather than incident frequency alone.

Systematic underreporting and data gaps warrant deeper examination. The observed incident trends likely reflect not only changes in threat activity but also variations in awareness, trust, and reporting behaviour. Future studies should investigate the drivers of underreporting, such as fear of reputational harm, uncertainty about legal obligations, limited detection capacity, or lack of incentives, and assess how these factors distort national cyber risk assessments. Such work would be critical to designing reporting frameworks that balance regulatory oversight with voluntary participation.

There is a clear opportunity to expand cyber victimology beyond gender-based analysis. While this report highlights gendered patterns of victimisation, future research could explore additional socio-demographic dimensions, including age, socioeconomic status, geographic location, digital literacy, and sectoral employment. Incorporating these variables would provide a more nuanced understanding of who is most at risk and enable more targeted awareness and protection programmes.

National cybersecurity capacity and skills gaps remain underexplored. Future research could assess the availability, distribution, and competencies of Jamaica's cybersecurity workforce across the public and private sectors, benchmarked against international standards. Understanding institutional and human resource constraints would help align policy recommendations with realistic implementation pathways and inform investments in education, training, and professional development.

A more detailed examination of the legal and regulatory environment would add significant value. While this report situates findings within a broad governance context, further research could analyse the effectiveness of existing cybercrime and data protection laws, enforcement mechanisms, and inter-agency coordination. Such analysis would clarify how legal frameworks shape reporting behaviour, victim protection, and deterrence, and identify areas requiring reform or harmonisation with international norms.

Future work could explore the role of public–private partnerships (PPPs) and multi-stakeholder governance models in greater depth. Given that much of the digital infrastructure and cyber risk exposure lies outside government, understanding how information sharing, joint response mechanisms, and trust-building arrangements operate, or could be strengthened, would provide actionable insights for national cyber resilience strategies.

Psychosocial and social costs of cyber incidents represent a largely unexamined dimension. Incidents involving cyber harassment, scams, and harmful content can cause psychological distress, erode trust in digital services, and affect social cohesion. Future interdisciplinary research integrating cybersecurity,

[20] C. Barclay, The Costs of Cybercrime and Data Breaches: Implications for Inclusive Growth in Jamaica, GIP Research Report 2026 (Forthcoming), https://www.pioj.gov.jm/

criminology, and social sciences would broaden policy responses beyond technical mitigation toward holistic resilience.

The relationship between technology adoption, digital inclusion, and cyber risk deserves explicit analysis. As digitalisation expands access to services and economic opportunity, it also alters exposure to cyber threats. Future research could examine how digital divides, based on income, geography, or skills, shape vulnerability and resilience, helping policymakers balance inclusion objectives with risk management.

Finally, there is scope for more systematic regional and international benchmarking. Future analysis could situate Jamaica's incident profile more explicitly within Caribbean and developing-country contexts. Such comparisons would support realistic target-setting, foster regional cooperation, and enhance Jamaica's engagement in international cyber capacity-building initiatives.

CONCLUSION

The analysis of cybersecurity incidents in Jamaica from 2021 to 2025 underscores the complex, evolving, and multi-dimensional nature of cyber risk. Cyber incidents affect individuals, public organisations, and private entities, highlighting the systemic and pervasive character of threats in both social and operational contexts. Individuals bear the majority of incidents, with women disproportionately affected, particularly in cases of fraud, online scams, harmful content, and social engineering attacks. Public organisations report the highest incident volumes, while private sector exposure is steadily increasing, driven by ransomware, data compromise, and fraudulent activity.

Key trends reveal that ransomware and social engineering are top vectors for organisational incidents, while fraud, harmful content, social engineering, and social media compromise dominate individual experiences. Emerging incident types, including misuse of personal information and other less-classified categories, point to the expanding threat landscape and the need for agile, adaptive risk management. Differential gender exposure, underreporting, and the persistence of high-impact but low-frequency incidents further emphasise the importance of targeted, evidence-based interventions.

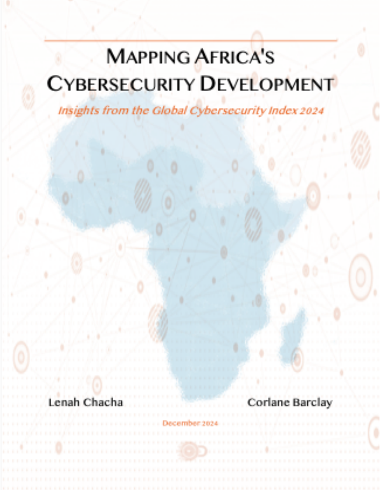
The findings highlight several critical lessons for national cyber governance:

1. Cyber risk is people-centred as much as it is technological, requiring investments in awareness, digital literacy, and human-focused mitigation strategies.
2. Trust, confidentiality, and legal clarity are essential to encourage reporting, particularly among SMEs and individuals, thereby improving threat visibility and enabling timely response.
3. Cross-sector collaboration between public institutions, private organisations, financial regulators, and law enforcement is essential to address high-volume, high-impact risks such as fraud and ransomware.
4. Systematic, standardised incident classification and reporting aligned with international norms is necessary to support trend analysis, policy evaluation, and resource prioritisation.
5. Cyber governance must integrate privacy, data protection, and cyber risk management, reflecting the interconnectedness of digital, economic, and societal impacts.

The Jamaican case illustrates that cybersecurity is a national resilience issue, not merely a technical challenge. Effective governance depends on evidence-driven decision-making, proactive capacity building, gender-sensitive strategies, and sustained collaboration across sectors. By leveraging incident data strategically, the country can strengthen prevention, preparedness, and response, ensuring that both individuals and organisations are better protected in an increasingly digital and interconnected environment.

DPO Caribbean Publications

Mapping Africa's Cybersecurity Development: Insights from the Global Cybersecurity Index 2024
ISBN 978 976 97440 1 1
https://dpocaribbean.com/publications



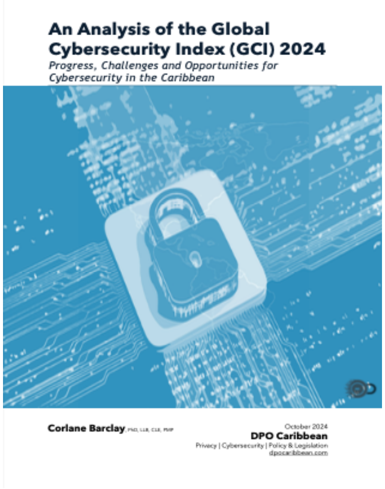
Mapping Africa's
Cybersecurity Development

Insights from the Global Cybersecurity Index 2024

Lenah Chacha
Corlane Barclay

December 2024

An Analysis of the Global Cybersecurity Index (GCI) 2024: Progress, Challenges and Opportunities for Cybersecurity in the Caribbean
ISBN 978 976 97440 0 4
https://dpocaribbean.com/publications



An Analysis of the Global Cybersecurity Index (GCI) 2024
Progress, Challenges and Opportunities for Cybersecurity in the Caribbean

Corlane Barclay, PhD, LLB, CLE, PMP

October 2024
DPO Caribbean
Privacy | Cybersecurity | Policy & Legislation
dpocaribbean.com

Jamaica Cyber Threat Report 2021-2025
Roadmap to Resiliency

DPO Caribbean
https://dpocaribbean.com/
20 West Kings House Road
Kingston, Jamaica, WI

9 789769 744028

ISBN 978 976 97440 2 8
Published in Kingston
Jamaica, WI, 2026